June 17, 2019

Donald Rucker, MD
National Coordinator for Health Information Technology
Office of the National Coordinator for Health Information Technology

Attention: Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2 Comments

Dear Dr. Rucker:

On behalf of iShare Medical, we applaud the ONC for its determination to find a solution to the complex problem of trust in healthcare interoperability. We would also like to thank the ONC for the opportunity to submit our comments on TEFCA Version 2. Our comments were prepared in conjunction with our response to the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule.

iShare Medical is developing a complete medical record organized around the person that is easily shared and becomes the foundation for a learning health system. We believe in that the bi-directional secure HIPAA compliant sharing of information among patients and HIPAA covered entities is critical to the ability for the U.S. to:

1) Improve care and outcomes
2) Reduce cost
3) Save lives

The following comments are on behalf of iShare Medical in response to:

Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2

Background

We believe that there has been significant change in HealthIT since the creation of the original version of TEFCA including:

- The advancement of FHIR and the call by CMS and ONC to develop FHIR API's
- Leveraging of DirectTrust Framework for transport of FHIR Messages to provide a bridge from where we are today e.g. DirectTrust Direct Messaging to the future FHIR API's

- Use of Certificates to digitally sign Jason Web Tokens (JWT) in real time thus allowing trust to be established in real time and creating scalable FHIR transactions

We believe that these advances in regulations, approach, and technology have not been fully incorporated into the proposed rule for TEFCA. Our response provides an approach that will incorporate a practical and scalable approach help the U.S. move from today's technology to future technology.

Executive Summary

We agree with the ONC that the problems around interoperability today are the result of lack of trust and anti-competitive behavior not technology. We agree that the patients' medical record should be available to the patient and their authorized users, their providers and the payers; however, we do not believe that the records follow the patient around from one system to another creating multiple duplicate copies.

We do not believe that TEFCA as written will solve these problems; however, we propose a solution that will solve these problems and achieve the following three high-level goals:

- A single "on-ramp" to nationwide connectivity
- Enable Electronic Health Information to securely be available to the patient and their authorized uses, their providers, and payers
- Support nationwide scalability

Single "On-Ramp" to Nationwide Interoperability

We propose a single on-ramp be achieved by requiring every entity including patients, the patients' authorized entities, providers, payers and their business associates that have access to or handle PHI and EPHI in health information exchange be Identity Proofed and assigned a trust credential that is bound to a digital identity. This "on-ramp" should also apply to app developers.

- We agree with the ONC that the level of Identity Proofing should be in accordance with NIST 800-63-3 Revision 3 at Identity Assurance Level 2 (IAL2).
- We agree with the ONC that the trust credential be bound to a digital identity bound to two key pairs (each key pair has one public and one private key) that complies with Public Key Infrastructure Certificate Internet X.509. Further, that each identity have two pairs of cryptographic keys, one pair is used for digital signature and the second key pair is used for encryption and decryption of data in accordance with FIPS 186.
- We agree that encryption and description should comply with FIPS 140-2 Level 2. Further, keys should be stored a Hardware Security Module providing both hardware and software encryption compliant with FIPS 140-2 Level 2.

Further, we propose that the digital identity contain the right to access authority such as:

- Patient Accessing Their Own Records

- Treating Provider
- Payer Responsible for Payment
- Business Associate of a Covered Entity

The requestor should be able to go directly to the source of the data and be trusted to get the data based upon their trust credential that is bound to their identity and their access authority. The trust credential would provide:

- Nonrepudiation of identity of the patient, provider, payer, or business associate
- Cryptographic certificate that is bound to that identity
- Right to access authority

Common Agreement Relationship to Patient and HIPAA

We propose the following solution: a patient should have a complete medical record organized around the person/patient (not their provider) that is easily shared with the patient, their authorized users, and HIPAA compliant entities. This can be achieved by having the provider push out to the patient medical record upon completion of the medical record in the EHR. This approach reduces the burden of query while still allowing all parties access to a complete medical record via notification of every change in the record. Each interested party, they patient, provider, and payer can indicate that they are an interested party with a HIPAA compliant right to the medical updates in the patient chart and be notified upon a change in the record.

With few exceptions, the patient has a right to their own medical record. HIPPA is the law that allows for access to medical records when the requestor is not the patient. There are three exemptions under HIPAA, they are for:

1. **Treatment:** The patient consents to treatment granting the treating provider the right to see their medical records. The treating provider exemption under HIPAA, allows the treating provider the right to access their patients' medical record so that they properly diagnosis and treat the patient. We believe that the treating provider should be able to see the records of other treating providers and add their medical record to the patients' complete medical record which in turn is then available to other treating providers. Each medical record should be locked such that no one can change a saved medical record. The data provenance of each update should be maintained and the patient should also be allowed to update their medical record. We believe that the patients shared medical record should be available to the treating provider as authorized by the patient.
2. **Payment:** The patients agree to assigns their benefits to the provider in a consent document referred to as "Assignment of Benefits Form". This form usually states that the patient agrees to assign their health insurance benefits to the provider which allows the provider the right to bill and get paid by the payer (insurer or government payer). This form also normally states that the patient agrees to allow the provider to share their medical records with the payer for the dates of service in which the payer is responsible for payment. This process grants the right of the provider to share medical records with the payer in pursuit of payment for a date of service. We believe that the patients' shared

medical record should be available to the payer for the dates of service to which the payer is responsible for adjudication of a claim as authorized by the patient.

3. **Operations:** HIPAA also recognized that the provider or payer might employ non-provider staff, contractors, companies, and other entities who might need to assist the provider or payer in the administrative aspects of running the provider or payer organization such as filing claims, copying medical records, performing prior authorization for services, adjudicating a claims and/or analyzing data. These entities are known as Business Associates. We believe that Business Associates should have the right to access medical records as delegated by the provider or payer under operations exemption under HIPAA.

Apps

There are many apps under development today. Most interfaces with HIPAA covered entities such as a provider or payer organization. We recommend that regardless of whether or not the app is required compliance with HIPAA that the HIPAA Security Rule, HIPAA Privacy Rule, HIPAA Brach Notification Rule, and HIPAA Enforcement rule be required. Further, we recommend that Apps be required to adhere with:

- Digital Identity and Two Factor Authentication in compliance with accordance with NIST 800-63-3 Revision 3 Identity Assurance Level 2 (IAL2)
- Trust Credential in accordance with FIPS 186
- Encryption and Decryption in accordance with FIPS 140-2 Level 2

Standard FHIR API's Should Not Cost to Connect

Some EHR vendors and HIE's view FHIR API's as a new source of revenue in which the EHR vendor or HIE can charge a fee for each API that connects to its EHR or HIE. The idea behind the FHIR API is to have a single universal plug in which all compliant FHIR API's can plug into and be instantly interoperable.

We are aware of charges ranging from a low of $1,000 to high as $30,000 per provider (customer of the EHR) to connect to the EHR.

For example assume that a vendor is designing a toaster to be used in the U.S. market. They can choose from many different types of electrical plug standards including ones used in the U.S. and Europe. The U.S. has standardized around a two or three plug connector. When a customer buys a toaster it works in every U.S. home. It would not make sense for this vendor to design any other plug except the one used for the U.S. Market for toaster build for the U.S. Market.

This is the way a FHIR API should work. It is a standard that plugs into every EHR, HIE, or App in the market. There is need to create a new plug. And, there is no need to charge each EHR, HIE, or each customer for the connection. The FHIR API should work regardless of provider, EHR, or care setting.

To be clear, we understand and agree that an EHR or HIE could incur cost that could be charged to the customer for other services such as training or a custom landing page, but the cost to connect should be minimal.

Provider National Wide Scalability

The use of digital certificates bound to identity with an trust authorization can provide for nationwide scalability by authenticating the person making the transaction and their trust credentials in real time.

Ask a QHIN / Push to a QHIN

There is no need for the complicated structure outlined in TEFCA. TEFCA proposes an approach based around the current HIE's infrastructure which is unnecessary complex. This approach calls for the requestor to ask the QHIN and that QHIN to ask another QHIN and for them to ask another QHIN until the information is found. This is a convoluted approach to finding the data – it like looking for a needle in a haystack. Further, there are no assurances that any QHIN will have the patients; complete medical record as patients move from one geographical area to another. We are also concerned that each chain in the QHIN process might request a processing fee which further increases cost and complexity. This process is not necessary if we are moving to a RESTful API approach.

Under a FHIR RESTful API, the parties can go directly to each others' address for bi-directional Exchange of health information. Trust is established by the trust credential or certificate that can sign the Jason Web Token (JWT) in real time. This approach works for both Query and Push notifications.

QHIN Message vs. Direct Secure Messaging

We disagree with the removal Direct Secure messaging from the 2015 Edition and the creation of QHIN Message. We believe that creating a new push messaging approach is not needed. Non-profit DirectTrust is the ANSI Accredited Standards Development Organization for Direct Secure Messaging. Further, we are concerned that the ONC may be under estimating how much Direct Messaging is being used in the backend of systems to power HL7 V2 ADT messaging, transitions of care, referral management, prior authorization for services, reporting to Registries and Federal Agencies, and support for CPC+.

In order to move forward, we need to build a path from the present to the future. We agree that FHIR is the next generation of interoperability; however, FHIR is not widely adopted today. EHR's are adding FHIR capabilities to their EHR's but this is a lengthy process. Only three of the top ten EHR's have more than single digit adoption rates of version 2.0 of FHIR (the current release of FHIR is version 4.0.0). The FHIR standard is moving quickly and will become the next standard, but please give the industry time to implement this standard.

Direct Secure Messaging; on the other hand, is the most widely adopted interoperability solution deployed today. Direct Secure Message is a part of every Certified EHR system which makes Direct Messaging the fastest way to deploy wide-spread interoperability.

DirectTrust Direct Secure messaging widely adopted and powering interoperability. DirectTrust has been experiencing exponential growth bringing nationwide interoperability to reality. DirectTrust reported first quarter 2019 results: 1.9 million DirectTrust Direct Addresses from 167k healthcare organization transacting 164 million transactions per quarter (55 million transactions monthly). Carequality, in contrast, reported per its website: 600k providers from 40k clinics and 1,400 hospitals. This comment is provided only as a reference to the volume of another organization and is not provided for any other purpose.

The non-profit DirectTrust is the largest health information exchange network in the U.S. and includes a diverse group of stakeholders as DirectTrust Accredited Trust Anchors and members who use the DirectTrust Direct standard for interoperability. DirectTrust's diverse members include, but are not limited to: insurers Anthem and UnitedHealthcare Group, EHR vendors Cerner, AllScripts, eClinical, Athena Health, and NextGen, e-prescriber SureScripts, pharmacy Walgreens, large healthcare organizations Intermountain Healthcare, Mayo Clinic, Baylor College of Medicine, Vanderbilt University Medical Center, and Trinity Health, State HIE's Hawaii Health Information Exchange, Michigan Health Information Exchange, and Wisconsin State Wide Health Information Exchange, associations American Academy of Dermatology, American Academy of Family Physicians, and two Federal Agencies the Indiana Health Services and the Veterans Health Administration. Further, DirectTrust recently created a sub-workgroup to discuss how Direct Secure Messaging can be used to speed the time it takes to get medical records for Social Security Disability claims.

Direct Secure Messaging is a standard for the secure bidirectional exchange of medical records nationwide. Direct Messaging can be used to transport any contents including CCD's, HL7 V2 messages, XDM/XDR, and images. Direct Secure Messaging has been implemented as a RESTful API using trigger events to automate processed including referrals, transitions of care, and HL7 V2 ADT (admission, discharge, transfer) message. This eliminates the need for healthcare providers to maintain connect via secure FTP (file transfer protocol) to transmit HL7 V2 ADT messages significantly reducing cost.

Direct Secure Messaging is a valuable interoperability solution that is currently experiencing exponential growth because Direct Messaging provides value to healthcare organizations and patients.

Removing Direct Secure Messaging from the 2015 Edition would be a major setback in achieving interoperability. We urge the ONC keep the Direct Secure Messaging in the 2015 Edition.

DirectTrust Direct Secure Messaging

What do you envision the rule of DirectTrust and Direct Messaging will play under TEFCA?

Provenance

We agree with the addition of data provenance. Further, we believe that patient generated health data as defined as data created by the patient outside of the provider setting including non-FDA approved devices, surveys, and reported outcomes should be included.

Patient Access

We agree that patients should be provided with timely access to their medical records. Further, we believe that patients have the right to access their entire or complete medical record. Currently patients are often limited to the data that the healthcare organization chooses to share with the patient and not their complete medical record.

Further, we believe that real-time access is possible. If you look at the financial industry such as online banking or online credit cards consumers have access to date in real-time. Therefore we believe that patients should have access to the complete (all the records at the provider or payer) in real-time. We recognize that providers must sign off on records before they can be made available to the patient.

We agree that patients should be able to export their data. Further, we believe that the export should be available in human readable and machine readable / structured format such that the records could be imported into an application program or EHR of another provider organization. There should be controls that prevent, detect and/or disclose records that have been changed or tampered with such as cryptographic keys that are "broken" when the record is modified.

Transitions Between HealthIT Systems

We strongly agree that health information should, upon the request of the patient/consumer flow freely between health care organizations regardless of care setting, provider or EHR system. Further, the patient should be entitled to their complete medical record.

We disagree that the HealthIT developer should have "flexibility as to how this is achieved". Instead we recommend that that HealthIT developer be required to use a standard format and content. This allows for all products to interoperate without the need to develop costly custom interfaces for each EHR or provider organization.

No EHI Outide of U.S.

We applaud the ONC is the new definition of EHI and the restriction of limiting access to EHI to inside the U.S. We know that U.S. computer systems and networks are under attack by entities outside of the U.S. who have no HIPAA compliant right to access. We believe that all EHI should be made available for interoperability among patients and HIPAA covered entities but restricted to the U.S.

We believe that there should be a standard for the content for export such that all developers can develop to this standard. For example, claims filed with insurers use the ASC 5010x12 standard, HL7 V2 messages, Direct Messages, and FHIR.

Security Labeling

We applaud the ONC is creating Security Labeling to sensitive data and data protected under SAMHSA. We feel strongly that the treating provider needs access to a complete medical record so that they can properly treat their patient. Not disclosing components of the medical record to the treating provider could cause preventable harm in that the provider might have made a different decision if all the information was known to the provider. That said, non-treating providers should not have access to this data without the consent of the patient.

Initial Step Persistent Access to All of the Patients EHI

We applaud the ONC in the requirement for persistent / continuous access to data. We recommend adding the words RESTful or REST. REST is an acronym for **RE**presntational **S**tate **T**ransfer. Here are six guiding principles of REST as defined by Roy Fielding, they are:

1. Client-server
2. Stateless
3. Cacheable
4. Uniform Interface
5. Layered System
6. Code on Demand

REST is an architectural style where data and functionality are considered to be resources. FHIR is an example of a RESTful API specification.

Encrypt Authentication Credentials

We support the use of encrypted authentication credentials in accordance with FIFS 140-2 Requirements for Cryptographic Modules. We believe that HealthIT vendors should be required to test to this requirement. Further, the cryptographic keys need to be bound to the entity of the entity to whom they belong such as these cryptographic keys can serve as nonrepudiation of identity for trusted exchange and create the trust framework for interoperability in accordance with NIST 800-63-3 Digital Identity Guidelines.

Multi-Factor Authentication

We support the use of Multi-Factor Authentication again bound to identity in accordance with NIST 800-63-3. This approach supports providence as we will know who did what, with what data, and when it was done.

Implementation with FHIR Standard

We support the adoption of FHIR Release 3 in accordance with the ONC's 2019 Interoperability Standards Advisory (ISA) recommendations; however, we do not support the removal of Direct Secure Messaging. Further, it might be helpful to create standards that evolve such as the most recently approved version of FHIR in which the ONC would update the version of FHIR that is required with a 12 month notification of the version to allow HealthIT vendors to program to the next version.

View Download and Transmit to a 3rd Party

We do not support the removal View, Download and Transmit to a 3rd Party. Removing Direct Secure Messaging and View Download and Transmit to a 3rd Party from the 2015 Edition would be a major setback in achieving interoperability. We urge the ONC keep the Direct Secure Messaging and View Download and Transmit to a 3rd Party in the 2015 Edition.

Integrating Revised and New Certification Criteria into the 2015 Edition Privacy and Security Certification Framework

We agree with the addition of privacy and security into the 2015 Edition. Further, we recommend that all HealthIT apps be required to implement privacy and security regardless of whether or not HIPAA applied to the HealthIT app (e.g. they are only a patient facing application).

New or Revised Certification Criteria in This Proposed Rule

We agree with the adoption of FHIR; however recommend the adoption of FHIR Release 3 instead of version 2 (the current release of FHIR is version 4.0.0); however, we do not support the removal of Direct Secure Messaging. Further, it might be helpful to create standards that evolve such as the most recently approved version of FHIR in which the ONC would update the version of FHIR that is required with a 12 month notification of the version to allow HealthIT vendors to program to the next version.

Information Blocking

We support that provision that HealthIT vendors, providers, and insurers should not engage in information blocking.

Security of HealthIT

We agree with the addition of privacy and security into the 2015 Edition. Further, we recommend that all HealthIT apps be required to implement privacy and security regardless of whether or not HIPAA applied to the HealthIT app (e.g. they are only a patient facing application).

Business Practices Related to Exchange

We agree that healthcare interoperability is critical to the future of health care. Interoperability is critical to improve care and outcomes, reduce cost, and save lives. Further, interoperability is necessary to support new payment modules such as value based care. That said, there is a cost to provide interoperability services and aggregate data to support clinical decision support and a learning health system. Fees related to these services need to be allowed in order to encourage innovation. Providing interoperability solutions is analogist to providing other forms of communications such as telephone and internet services.

Apple

It has been pointed out that Apple has implemented FHIR. Further, there has been an implied that having medical records on your iPhone is "free". Apple is an $800 Billion company that has developed a proprietary product that works exclusively on Apple IOS. Using an Apple phone is not free. An iPhone version 8 which is the minimum version that support medical records costs at least $300 and a services contract costs at least $50 per month. Apple is a well-respected company but make no mistake that there is a cost to having an iPhone and medical records on your iPhone is a proprietary application.

FHIR vs. SMART of FHIR

SMART "Substitutable Medical Applications, Reusable Technologies" was created in 2010 by a $15 million grant from the ONC. SMART is managed by Boston Children's Hospital Computational Health Informatics Program and the Harvard Medical School Department of Biomedical Informatics. SMART initially started out defining content of a medical record. SMART is not an ANSI Standards Development Organization.

FHIR "Fast Healthcare Interoperable Resource" was also under development by HL7 "Health Language Seven International". FHIR is an international standard that defines the structure and content of the medical data. FHIR continued to gain world-wide support as the next generation of content standards in healthcare. FHIR is a ANSI Standards Development Organization.

In 2013, SMART decided to pivot to focus on the creating an application layer on top of FHIR known as SMART on FHIR. SMART on FHIR is designed to allow EHR's and health system to choose how applications will interact with data contained in EHR systems. SMART on FHIR allows health systems to choose:

1. Who the EHR and/or health system is willing to share data or which applications will be authorized to have access
2. What data elements will be shared with the application
3. How the data will be shared with the application. To date, all SMART applications have been implemented to be "read only access" and do not allow for bi-directional sharing of data. Further to date most applications using SMART are limited to research-based applications.

SMART is an additional application layer in front of the EHR that is designed to allow health systems the ability control of who, what, and how applications can access the data contained within their EHR system.

SMART uses OAuth2 which works like this: the system that controls the API and data is called the resource server and the server checking authorization is called the authorization server (note they don't have to be separate systems just separate functions). How these two servers interact is not defined in the specification so it is up to each EHR to define. Authorization can be provided by a token or via identification of the user and permission via a cryptographic key.

We are concerned that SMART on FHIR could provide another way for EHR's and health systems to continue data blocking. Further, we are concerned that SMART on FHIR could be biased because it is governed by a healthcare provider organization and not a diverse group of stakeholders. We believe that governance should be via a conscious group similar to HL7 and DirectTrust.

HIPAA Compliant Democratization of Data

What is needed is HIPAA compliant democratization of data by allowing access to patients and HIPAA Compliant entities via standard process that is specified. This means:

1) Every FHIR client application can communicate with every FHIR server application using a standard specification
2) Access to data is based on the credentials of the requestor. These credentials should be bound to the identity of the entity making the request such as patient, healthcare provider, insurer, or device which is bound to a token or cryptography keys that provide non-repudiation of identity.
3) Right to access authorization authority:
    a. Patient or their delegated entity accessing data on behalf of the patient
    b. HIPAA compliant covered entity / treating provider
    c. HIPAA compliant health insurer
    d. HIPAA compliant business associate of a covered entity who meets the definition of operations

This removes the ability of an EHR vendor or provider organization from blocking access to data from individuals or entities to that have the right by virtue of being a patient or granted under HIPAA to access the data.

Further, we believe the DirectTrust Trust Framework for identity proofing and assignment of cryptographic keys can be leveraged to create the trust framework for FHIR by digitally signing the Jason Web Token (JWT) in real time thus establishing trust between to previously unknown entities.

Principles for Trusted Exchange

There are six principles outlined in TEFCA. The following is a list of the six principles and our response:

- Principle 1 – Standardization: Adhere to industry and federally recognized standards, policies, best practices, and procedures.

  We strongly support the use of standards.

- Principle 2 – Transparency: Conduct all exchange and operations openly and transparently.

  We support transparency and non-discrimination. A HIN must allow participation by providers and payers(e.g. covered entities), and patients and their authorized users.

- Principle 3 – Cooperation and Non-Discrimination: Collaborate with stakeholders across the continuum of care to exchange EHI, even when a stakeholder may be a business competitor.

  We agree that information should flow freely and that the HIN should not engage in data blocking. Further, we believe that a condition of participation should not be the requirement to pay a unreasonable large fee that could in and of itself provide a barrier to participation and a form of discrimination.

- Principle 4 – Privacy, Security, and Patient Safety: Exchange EHI securely and in a manner that promotes patient safety, ensures data integrity, and adheres to privacy policies.

  We agree with the requirement for a HIN to conduct patient safety and identity management. The use of a trust credential bound to two pairs of cryptographic keys provide for non-repudation of ident of identity. There is no need for patient matching if identities are bound to a cryptographic key as the key provides a 100% match every time.

- Principle 5 – Access: Ensure that individuals and their authorized caregivers have seamless access to their EHI.

  We applaud the ONC in making health information available to the patient and their care givers. Item 2 states: "(2) enable individuals to direct their EHI to any desired recipient they designate" we wanted to clarify that a patient may have more than one recipient and that the recipient can be a provider, payer, business associate or caregiver. Further, we encourage the ONC to require the content to be standards-based electronic copy of their health record be shared with one or more providers, payers, business associates or caregivers that they designate.

- Principle 6 – Population Level Data: Exchange multiple records for a cohort of individuals at one time in accordance with applicable law to enable identification and trending of data to lower the cost of care and improve the health of the population.

  We agree that the ability to push batches of data is desirable; however, each individual record within the batch must meet the requirements under HIPAA and be at the request of the patient, HIPAA Covered Entity, or their the Business Associate of a covered entity. Further, the best way to implement push batches of data is through Direct Messaging in a secure trust framework DirectTrust Direct Messaging.

QHIN

By definition QHIN's must support the iHE technology. This is inconsistent with CMS goals to promote interoperability through the use of FHIR API's. The purpose of TECFA was to fix the failed system of HIE system which creates a small set of data that has not been easily shared or available to providers, payers, and patient and their care givers.

The QHIN approach outlined in TEFCA creates geographically defined regions controlled by HIE's. Patient that move from one State to another will need to create a broadcast query could generate 10's of 100's queries to get access to their data.

We need to innovate the future. Think differently. What has failed us in the past? Redundant, fragmented data, stored in silos that are not easily shared. What are we proposing in TEFCA? Redundant, fragmented data, stored in silos that might be easier to share. But fundamentally it's the same redundant, fragmented data story. What do we need. We need to think differently. We need to store the medical records around the person not the provider. One cradle to grave lifetime medical record that can get retrieved, added to and shared maintained by a records custodian who keeps the records up to date.

We recommend that the ONC consider other platforms such as Direct and FHIR that could also be a QHIN.

* * * * * *

Thank you for this opportunity to share our input and look forward to the Final Rule.

Sincerely,

Linda Van Horn, BS, MBA
President / CEO
iShare Medical